ICST Transactions
on Security and Safety

Research Article ICST.ORG

Trust in social computing
The case of peer-to-peer file sharing networks

Heng Xu[1], Tamara Dinev[2], Han Li[3,*]

[1]College of Information Sciences and Technology, Pennsylvania State University, University Park, PA 16802, USA; [2]Barry Kaye College of Business, Florida Atlantic University, Boca Raton, FL 33431, USA; [3]School of Business, Minnesota State University, Moorhead, MN 56563, USA

Abstract

Social computing and online communities are changing the fundamental way people share information and communicate with each other. Social computing focuses on how users may have more autonomy to express their ideas and participate in social exchanges in various ways, one of which may be peer-to-peer (P2P) file sharing. Given the greater risk of opportunistic behavior by malicious or criminal communities in P2P networks, it is crucial to understand the factors that affect individual's use of P2P file sharing software. In this paper, we develop and empirically test a research model that includes trust beliefs and perceived risks as two major antecedent beliefs to the usage intention. Six trust antecedents are assessed including knowledge-based trust, cognitive trust, and both organizational and peer-network factors of institutional trust. Our preliminary results show general support for the model and offer some important implications for software vendors in P2P sharing industry and regulatory bodies.

Keywords: network-based community, peer-to-peer (P2P) file sharing, risks, social computing, trust

Received on 15 February 2011

doi: 10.4108/icst.trans.secsafe.2011.e5

1. Introduction

New applications and services that facilitate user collective action and social interaction with rich data exchange have been driving a dramatic evolution of the Web [1, 2]. Examples include blogs, wikis, social bookmarking, user-driven ratings, peer-to-peer (P2P) networks, photo and video sharing communities, and online social networks. In the literature, these applications or services have been variously referred to as *social computing*, which reflects the increased role of computing in social structures, in empowering individual users and communities and not just institutions [1, 3]. Social computing platforms share several features that differentiate them from traditional organizational computing and content sharing. Specifically, these platforms tend to be decentralized, dynamic, and flexibly structured in terms of how information is gathered and distributed [1, 3].

Social computing is seen as having a profound impact on the global economy both through impacting the social structure [4] and the technology development as a whole [2]. In terms of social structure, individuals increasingly take cues from one another rather than from public or private organizations such as corporations, media, religion, and political institutions. Charron *et al.* [4] point to several important tenets driven by the social computing: innovation shift from top-down to bottom-up; value shift from ownership to experience; power shift from institutions to communities. In terms of IT developments, social computing seeks to improve social software that can facilitate interaction either between groups or individuals and computing tools.

The above-mentioned innovation, value, and power shift from organizations (which represent an identifiable and law-bound entity) to communities informs also a shift in risk and trust perceptions and their importance to the community members. As Parameswaran and Whinston [1] pointed out, social computing platforms empower 'individual users with relatively low technological sophistication in using the Web to manifest their creativity, engage in social interaction, contribute their expertise, share content, collectively build new tools, and disseminate information and propaganda' (p. 763). In these platforms users

*Corresponding author. Email: li@mnstate.edu

routinely engage with a large number of user communities with whom they have little or no prior interaction. This exposes users to an even greater risk of opportunistic behavior by malicious or criminal communities that can make use of the anonymity, fault tolerance, robustness, and low cost of online communities to build platforms for illegitimate interaction, communication, and data exploration [1]. Given that users face realistic concerns pertaining to social computing, we seek in this paper to understand what steps can be taken to increase users' trust perceptions and reduce their risk perceptions so as to encourage legitimate interactions in social computing platforms.

Trust is a crucial enabling factor in relations where there are uncertainty, interdependence, risk, and fear of opportunism [5, 6]. Little is known, however, regarding how trust beliefs are formed and developed in terms of using social computing applications, and what individual, organizational, and community factors influence the trust formation. Following the conceptual and integrative development of trust in the field of Information Systems, we develop and empirically test a research model that incorporates multiple, interrelated factors contributing to the formation of trust beliefs in the context of P2P networks. With specific reference to P2P networks as a social computing platform, such environment facilitates the development of communities through the creation of 'architectures that allow peer-wise communication and social action'. In developing the research model, we identify new trust-building mechanisms, namely peer-network situational normality and peer-network structural assurances. These peer-network structures would be especially suited for network-based virtual community such as P2P networks, constituted by individuals with unstructured and non-static relationships, interacting together in a community [7].

Moreover, it has been noted that the openness of P2P networks that renders them advantageous can also be a liability in terms of attack vulnerability [8]. Given these potential liabilities, 'in the social platforms, reputation and trust will be key determinants' in their usage [1, p. 774]. Such concerns certainly support the study of trust and perceived risk in P2P networks. In current research, we developed a trust-risk model and empirically tested our model with a survey of 136 experienced and voluntary P2P users in a large university in Singapore. By rigorously specifying the antecedents of trust beliefs, our objective is to conceptually clarify and verify the multiple factors that inform trust formation in social computing context. In what follows, we first describe the theoretical foundation that guides the development of the research model. Then we develop the research hypotheses that identify factors included in the process wherein individuals form trusting beliefs. This is followed by the research methodology and findings. The paper concludes with a discussion of the results, the practical and theoretical implications of the findings, and directions for future research.

2. Theoretical foundation and research hypotheses

2.1. P2P networks

Peer-to-peer (P2P) networks consist of nodes communicating directly for the purpose of exchanging content files, with no centralized governing node [9]. Each participant in the P2P network can behave either as a client, receiving files, or as a server, sending files, or both [see 8 for a review]. Users need to run specific P2P sharing software on their local computers in order to participate in the P2P network. P2P sharing software, in this study, is defined as an application running P2P sharing technology dedicated for searching, downloading, and sharing digital resources among peer users (peers), such as file sharing software like Gnutella and KaZaA, and CPU sharing software like SETI@home. While the term P2P is widely associated with sharing of music and movies that often involve copyright violations, its scope is far wider which can be used to exchange any digitized content [8]. Parameswaran and Whinston view P2P software as 'social software taken to the extreme, bypassing limitations of the browser interface and the DNS (Domain Name System) addressing, radically decentralized, and relying almost exclusively on collective action by users at the edge' (p. 765).

Given the current existence of various uncertainties in P2P sharing such as resource piracy [10], computer attack by malicious peers [11], and privacy invasion [12–14], it is crucial to understand the factors that will affect individual's usage of P2P sharing. In this study, we only focus on examining the voluntary use of P2P sharing software, free of charge. Non-voluntary use of P2P sharing often happens within organizations and such a case is not the focus of current research. Furthermore, we focus on those P2P sharing networks where all peers are equal and anonymous[1] [12], without central administrators or power peers who have the capability to control other peers. Throughout the rest of the paper, we use the following terms: *resources* referring to files or computer hardware being shared out; *resources download* referring to retrieving resources from other users' computer over the Internet; *sharing resources* referring to allowing others to access and download the shared resources; *vendor* referring to the producer of P2P sharing software; *peer* is used in exchange with the term *user*; *peer network*, or *P2P sharing*

[1]Reiter and Rubin (1999) conceptualized three degrees of anonymity: (i) type, which states sender or receiver anonymity; (ii) adversary, or who is trying to break the anonymity, and (iii) degree, which may range from absolute privacy (imperceptible presence) to possible innocence, to exposed (to the adversary), to provably exposed (to others). In P2P sharing, peer anonymity is referred to as a peer's identity hidden from other peers (type), but with the possibility of being exposed to a malicious peer (adversary and degree).

network, is the network of peers running the same P2P sharing software.

2.2. Risks in P2P file sharing

Risk has been generally defined as the uncertainty resulting from the potential for a negative outcome [15] and the possibility of another party's opportunistic behavior that can result in losses for one self [16, 17]. Perceived risks affect an individual's intention and actual usage of a technology especially in a high uncertain environment, such as online shopping [18]. An individual's calculation of risk involves an assessment of the likelihood of negative consequences as well as the perceived severity of these consequences [19]. The negative perceptions related to risk may affect an individual emotionally, materially, and physically [20].

In the P2P sharing context, a user could be exposed to uncertainties related to three sources: *peers* (including the user herself), the *vendor of the P2P sharing software,* and *the Internet*. The user, therefore, may perceive that there is some probability of suffering a loss when downloading or sharing resources in the P2P network. For example, a peer may find her computer overloaded or attacked by malicious peers (peer-related performance risk); she may face legal suit or even jail (legal risk) when she shares pirated resources with other peers [10]; she may by mistake share her entire hard disk or other principal data repository as material available to others (peer-related privacy risk). Moreover, the user may not be informed of her online activities being disclosed to third parties by the software vendor (vendor-related privacy risk) [13]. A peer may find the software's performance is not as good as expected, or hard to find and download her intended resources (vendor-related performance risk). Furthermore, the data transmission over Internet incurs potential channel risk as the attacker might be an eavesdropper that can observe some or all messages sent and received over the Internet [21]. Without proper control of the risk in P2P file sharing, a user may choose not to use the software due to high risks [22]. For example, Pavlov and Saeed [23] reported that the deteriorated performance of Gnutella software often causes failed download and leads users to give up the usage. In this study, we define a user's perceived risks in using P2P sharing software as the user's perceived probability of suffering a loss when downloading or sharing resources in the P2P network.

2.3. Trust

Trust has received a great deal of attention from scholars in the disciplines of social psychology [24], sociology [25], management [26], and marketing [27]. In examining the published literature on trust, various definitions of trust have been proposed in many different ways. Nevertheless, across disciplines there is consensus that trust is a crucial enabling factor in relations where there are uncertainty, interdependence, risk, and fear of opportunism [5, 6]. 'The need for trust only arises in a risky situation', and trust could be an effective mechanism to reduce the complexity of human conduct in situations where people have to cope with uncertainty [28]. Trust involves at least two entities in relation to each other—a trustor and a trustee. In e-commerce, the consumer is usually seen as the trustor, the party who places him or herself in a vulnerable situation; and the e-vendor is the trustee, the party in whom trust is placed and who has the opportunity to take advantage of the trustor's vulnerability [29].

Before engaging in a discussion of trust, it is helpful to delineate the differences between trust belief and trust intention. Trust belief, on the one hand, is the trustworthiness perception of certain attributes specific to a *trustee*, while trust intention, on the other hand, is the psychological state of a *trustor*, i.e. trustor's intention to engage in trust-related behaviors with a specific trustee. Even though efforts have been devoted to differentiating trust belief from trust intention [see 30, 31], most researchers adopted the conceptualization of trust as a set of specific *trust beliefs* in e-commerce studies [32, 33]. Consequently, this study has adopted the conceptualization of trust as three specific beliefs that are utilized most often [31, 33, 34]: competence (ability of the trustee to do what the trustor needs), benevolence (trustee caring and motivation to act in the trustor's interests), and integrity (trustee honesty and promise keeping).

In the context of P2P file sharing, because of the absence of proven guarantees that the vendors and other users or third parties will not engage in harmful opportunistic behaviors, trust is crucial in helping users overcome their perceptions of uncertainty and risk [18, 35]. Research has shown that vendors' trustworthiness attributes are important to users. Lee [36] found that the four out of the top 10 most important features in P2P sharing software rated by users are related to trust, including 'stability', 'reliability' (competence), 'can exit nicely' (integrity), and 'gives error message' (benevolence). Tsivos *et al.* [13] also proposed that P2P sharing systems should have built-in self-regulatory characteristics to reduce the complexity of uncertainty, including characteristics such as stopping queries that are bound to match too many files and eliminating duplicate packets from overzealous users. Following trust definition in e-commerce and other contexts [16, 32, 37], we define *trust of P2P vendors* as a set of *specific beliefs* dealing primarily with the integrity, benevolence, and competence of vendors. Lack of trust and high risks (e.g. security risks and legal risks in terms of copyright infringement) have seriously undermined the development of consumer-friendly P2P business initiatives [8].

Three types of trust antecedents will be examined in this research: institution-based trust (specifically, structural assurance beliefs and situational normality beliefs),

knowledge-based trust (specifically, direct knowledge of or experiential interaction with a trustee), and cognition-based trust (specifically, reputation categorization process). Figure 1 presents our research model. The following sections develop and elaborate the key constructs and the theoretical rationale for the causal relationships among the constructs in the research model.

2.4. Knowledge-based trust

Familiarity with vendors comes from prior first-hand experience. It is suggested that familiarity builds trust in *a priori* trustworthy party [38] and validated in e-commerce context [32]. Familiarity with vendors is different from situational normality because the latter does not involve the knowledge about the actual vendor [32]. In the context of P2P file sharing, familiarity with a vendor, e.g. refers to how knowledgeable a user is about the procedures and techniques for performing P2P sharing activities.

It is suggested that trust in an *a priori* trustworthy party grows as the trust-relevant knowledge is accumulated from experience with the other party [24]. In e-commerce, familiarity with e-vendors is found to lead to higher trust beliefs in vendors [32]. In the context of P2P file sharing, trust-relevant knowledge that is derived from prior experiences, such as the procedures and techniques for performing P2P sharing activities, should help the development of trust in the software vendor. Therefore, we hypothesize:

H1: Familiarity with the vendor of P2P sharing software positively affects trusting beliefs.

2.5. Cognitive trust

Cognition-based trust is formed *via* categorization processes in which individuals place more trust in people similar to themselves and assess trustworthiness based on second-hand information and on stereotypes [30, 32]. Prior research considers reputation as an important subcomponent of the cognitive trust and suggests that a trustor may categorize a trustee as trustworthy or untrustworthy based on the reputation of the trustee [30]. The reputation categorization process infers that a trustee with a good reputation is believed to be trustworthy [30]. Therefore, if the trustee has a good reputation, trustor will quickly develop trusting beliefs about the trustee, even without first-hand knowledge or direct experiential information [30, 39]. Thus, in the context of P2P sharing, we predict that vendors with a good reputation are seen as trustworthy and those with a bad reputation as untrustworthy.

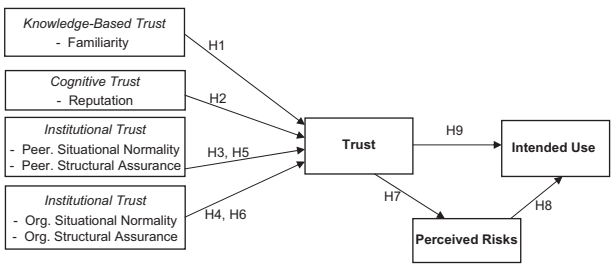

Figure 1. Research model.

H2: Reputation of the vendor of P2P sharing software positively affects trusting beliefs.

2.6. Institutional trust

Institution-based trust means that 'one believes that the necessary impersonal structures are in place to enable one to act in anticipation of a successful future endeavor' [30, p. 478]. Among the above-mentioned trust antecedents, institution-based trust is consistently found to have positive impacts on the development of trust in e-vendors for both experienced [32] and inexperienced users [18, 31, 40]. Institutional trust is one's perception of the existence of guarantees, safety nets, or other impersonal structural conditions to facilitate achieving the expected outcomes [41, 42].

Prior research examining the institutional trust in information systems has mostly focused on a single institutional context in the electronic market environment—the organizational context [33]. However, when studying trust in social computing, we believe more complex institutional contexts should be considered. For example, in a P2P environment, two sets of structures are involved in forming users' trust beliefs—the organizational structures and the peer-network structures. We refer the organizational structures to a user's perceptions of the institution environment of a P2P sharing network. Influential factors in forming users' trust beliefs include the organizational resources and procedures, vendor guarantee such as the code of conduct of P2P United [43], the association of P2P software vendors like BearShare, Grokster, and eDonkey, which regulates member vendors in terms of user privacy, security, and respect for copyright laws. In the light of frequent calls for self-regulations among P2P sharing vendors [23], it is important for us to examine the impacts of these organizational structures.

We further believe that the peer-network structures would be the other important factor in forming users' trust beliefs. In a P2P network, trust of a peer is hardly developed because trust is often applicable to a relationship with another *identifiable* party [44] and a peer can easily hide her identity from others. Thus, peers' behaviors such as free-riding shared resources can deteriorate the performance of a P2P sharing network and thus negatively impact others' sharing activities [23, 45]. This is not surprising as in P2P networks, both cooperative and non-cooperative

behaviors are facilitated given the decentralized nature of such networks [46]. Moreover, there are reports that P2P networks are inserted with low-quality or damaged versions of music files for various purposes [47, 48]. Also P2P networks are criticized being utilized for exchanging pirated resources among some peers. These uncertainties in peer-network may expose users to various risks and drive them to withdraw from the use of P2P sharing software [22]. Consequently, we propose a new dimension in institutional trust, namely *peer-network structure*, relating to one's perceptions that other users on the same peer-network appear to be normal or favorable and the P2P sharing actions are likely to incur low risk.

Existing research on institutional trust has focused on the organizational structure in the context of electronic markets [5, 31, 32, 49, 50]. However, as a specific attribute of network-based virtual communities in social computing, peer-network structure should be explicitly conceptualized as one type of institutional trust that is distinct from the organizational structure. When the network of relationships in network-based virtual community is unstructured and non-static, it is especially important for participants in such network to recognize that the peer network they are interacting with is of low-risk [cf. 7]. At the same time, peer-network structure is distinct from knowledge-based familiarity with a P2P vendor, or cognitive-based trust, in two ways: (i) the peer-network structure is the perception about collective peers who may not be identifiable and (ii) the perceptions of peer-network structure can be derived from first-hand experiences of using the particular P2P sharing software, second-hand information such as news from media, or a combination of both. In current research, we believe a thorough investigation of both peer-network and organizational institutional contexts will improve our understanding of trust-risk model in social computing.

There are two components of institutional trust discussed in the literature: (i) situational normality, defined as the belief that the situation appears to be normal or favorable and success is likely [51] and (ii) structural assurances, defined as the belief that success is likely because such contextual conditions as promises, contracts, regulations, and guarantees are in place [30].

Situational normality. Situational normality stems from the belief that the environment is in proper order [25] and success is likely because the situation is normal or favorable [51, 52]. Situational normality could be related to a greater trust belief because it assures people that everything in the setting is as it ought to be [30, 42] and thus their interactions with others in this setting are in accordance with what they consider to be anticipated [32]. When people face unanticipated or abnormal situations, they are uncomfortable and tend to not trust others in this kind of setting [39]. Empirical studies in e-commerce context have generally supported the positive impacts of situational normality on trust [31, 32] and operationalized situational normality by referring to the trustee being studied, e.g. a specific online vendor or a particular web site. In current research, we operationalize two situational normality constructs: organizational and peer-network situational normality. Situational normality in the peer-network context is operationalized with collective peers who share or download resources on a P2P network. Users are more likely to have positive trusting beliefs if they believe that majority of peers are interacted in a predictable and reliable manner. Therefore, we hypothesize:

H3: Peer-network situational normality positively affects trusting beliefs.

Situational normality in the organizational context is operationalized with vendors of P2P sharing software. Users are more likely to have positive trusting beliefs in a P2P vendor if they observe that the P2P sharing software has a typical user interface, a set of expected procedures, and a typical set of functionalities for P2P sharing activities based on their knowledge and experiences of other similar P2P sharing software. For example, a number of P2P software encourages users to share their resources by offering some rewards, e.g. the more being shared, the faster download a peer can enjoy. As a result, a user would expect such a rewarding mechanism to be built in the P2P sharing software and tend to build trust into the vendor if the vendor provided such functionality. Therefore, we hypothesize:

H4: Organizational situational normality positively affects trusting beliefs.

Structural assurances. Structural assurances refer to the beliefs that structures like regulations, guarantees, and legal resources could guide, empower, and constrain the conduct of individuals and organizations [30, 31, 53]. Examples of structural assurances built into the Web environment could include regulatory or watchdog agencies, legal resources, seals of approval, explicit privacy policy statements, guarantees, affiliation with respected companies, and special interest groups such as consumer or trade associations [5, 32, 54]. Similar to situational normality, two structural assurance constructs were operationalized in current research: organizational and peer-network structural assurances. In a peer-network context, techniques such as reputation building, prevention of pirated resources from being injected into P2P network, and risk reduction mechanisms like anti-flooding and anti-attack have been proposed and implemented into P2P sharing software [55, 56]. These peer-network structures can prevent opportunistic behaviors of peers [57] and thus can build user confidence and trust in the P2P systems

and their vendors. Thus, users who perceive high peer-network structural assurances would attribute this to the competence and integrity of the system and thus increase trust in the vendor. Therefore, we hypothesize:

H5: Peer-network structural assurance positively affects trusting beliefs.

In the context of e-commerce, it has been found that organizational structural assurance could limit the firm's ability to behave in negative ways, allowing consumers to form and hold beliefs about expectations of positive outcomes [58]. When violation occurs, these structures could provide mechanisms of voice and recourse [30, 58], which could create strong incentives for firms to refrain from opportunistic behavior and behave appropriately. For example, industry self-regulation body such as P2P united, created code of conduct which regulates member vendors in areas such as users' privacy, security, and respect for copyright laws. Users should be more inclined to trust vendors who are members of P2P United due to the statements of guarantees. Besides these, safety guards such as vendor's privacy statement could also lead to higher trust in vendors. Hence, we hypothesize:

H6: Organizational structural assurance positively affects trusting beliefs.

2.7. Trust, perceived risk, and intended use

The effect of trust on risk reduction has been empirically supported in e-commerce context [18, 21, 35, 59]. Trust could reduce information complexity and lower the perceived risk of a transaction. It has been established in e-commerce that trust in an e-vendor reduces the level of perceived risk [18]. Based on these findings, in the context of P2P sharing, we propose that trusting beliefs in vendor's attributes such as competence, benevolence, and integrity should lower users' risk perceptions in P2P sharing. With the trusting belief in the vendor's capabilities, a user may perceive a lower level of risk such as privacy invasion, free-riding, virus attack, and injection of pirated resources, etc. Hence, we hypothesize:

H7: Trusting beliefs reduce perceived risks in P2P file sharing.

Along the line of Theory of Reasoned Action [60, 61], risk perception viewed as the negative antecedent belief, and trust viewed as the positive antecedent belief, could both affect a person's attitude that in turn influence a person's behavioral intention [18]. Empirical evidence supports the above expectations of the negative relationship between perceived risk and behavioral intention, and the positive relationship between trust and behavioral intention in e-commerce context [62, 63]. We suggest that the same logic can be extended to P2P sharing context and thus we hypothesize:

H8: Perceived risks in P2P file sharing decrease intended use of P2P sharing software.
H9: Trusting beliefs increase intended use of P2P sharing software.

3. Research method

3.1. Instrument development

Measurement items were developed based on procedures advocated by Churchill [64] and Moore and Benbasat [65]. As far as possible, constructs were adapted from existing measurement scales used in prior studies to fit the context of P2P file sharing where necessary. All the constructs are operationalized as reflective constructs, and adapted from prior trust literature with modifications to reflect the specific context of the P2P sharing in the survey questions. *Intended use* was measured with three items asking the extent to which users would reuse the P2P sharing software [33]. Measures of *perceived risks* were based on the measures used in Pavlou and Gefen [33], adapted to refer to the expectation that a high potential for loss would be associated with the use of P2P sharing software. *Trusting beliefs* were measured with three items that were directly taken from Gefen *et al.* [32]. The measures for *reputation* were developed based on a review of reputation-based trust [31, 50]. These items generally referenced a vendor having an overall good reputation [31]. *Familiarity* was measured by three items based on Gefen *et al.* [32]. In terms of *institutional trust*, measurement for organizational situational normality and structural assurance was adapted based on the measurement of trustworthy attributes of a vendor in Gefen *et al.* [32]; measurements for peer-network situational normality and structural assurance were adapted from the measurements of institution-based trust in McKnight *et al.* [31]. All items in the questionnaire were anchored on 7-point Likert scale. Appendix A presents the final questions measuring each construct in this study.

3.2. The survey

To examine the effects of perceived risk in P2P sharing and trust in vendors on the intention to use P2P sharing software, a survey technique was employed. Email addresses of 600 undergraduate students were randomly collected from an online learning system at a large university in Singapore. Invitation emails explained the purpose of the study and stated that only those who have prior experience in P2P sharing were eligible to participate in the online survey. Also included in the invitation emails was the URL link to the Web-based survey

questionnaire. The respondents were told that their anonymity would be assured and the results would be reported only in aggregate. As an incentive for participation, three monetary awards of Singapore dollar $40 per person[2] were raffled among the participants.

To ensure that the data are collected among experienced users of P2P sharing software, respondents were requested to complete the online questionnaire by answering the questions regarding the recent P2P sharing software which they used for resource searching, download, or sharing. Respondents were also required to indicate the name of that P2P sharing software and the usage frequency during past three months. Questionnaires from respondents who had not indicated the previous usage of P2P sharing software were discarded. A total of 136 responses were resulted. The mostly used software applications from the respondents were KaZaA (72%), BitTorrent (12%), Emule (9%), and Shareaza (6%).

4. Data analysis

A second-generation causal modeling statistical technique—partial least squares (PLS), was used for data analysis in this research for three reasons. First, PLS is widely accepted as a method for testing theory in early stages, while LISREL is usually used for theory confirmation [66]. Thus PLS is more suitable for our exploratory study. Second, PLS is well suited for highly complex predictive models [67]. Prior research that applied PLS [68] has claimed that it is best suited for testing complex relationships by avoiding inadmissible solutions and factor indeterminacy. This makes PLS suitable for accommodating the relatively complex relationships among various constructs in this research. Third, PLS has the ability to assess the measurement model within the context of the structural model, which allows a more complete analysis of interrelationships in the model.

4.1. Testing the measurement model

The measurement model was evaluated by examining the relationships between the constructs and the indicators. Such examinations may include the test of the convergent and discriminant validity of constructs. Three tests are used to determine the convergent validity [69]: reliability of questions, the composite reliability of constructs, and the average variance extracted by constructs. Reliability of these questions was assessed by examining the loading of each question on the construct. In order for the shared variance between each question and the construct to exceed the error variance, the reliability score for the question should be at least 0.707 [70]. Given that all questions had reliability scores above 0.707 (see Table 1), the questions measuring each reflective construct had adequate reliability. Composite reliabilities of constructs with multiple indicators exceeded Nunnally's [71] criterion of 0.7 while the average variances extracted for these constructs were all above 50% and Cronbach's alphas were also all higher than 0.7. Overall, the above test results indicate that the convergent validity of all constructs is adequate.

Discriminant validity is the degree to which measures of different constructs are distinct [72]. To test discriminant validity, the squared correlations between constructs (their shared variance) should be less than the average variance extracted for a construct. Table 2 reports the descriptive statistics and the results of discriminant validity, which is checked by comparing the diagonal to the non-diagonal elements. All items fulfilled the requirement of discriminant validity.

4.2. Testing the structural model

After establishing the validity of the measures, we tested the structural paths in the research model using PLS. We conducted hypothesis tests by examining the sign and significance of the path coefficients. A jack-knife resampling technique was applied to estimate the significance of the path coefficients. Given that each hypothesis corresponded to a path in the structural model, support for each hypothesis could be determined based on the sign (positive or negative) and statistical significance for its corresponding path. Figure 2 shows a graphical display of the results of hypothesis testing. The explanatory power of the structural model is assessed based on the amount of variance explained in the endogenous construct (i.e. intended use). The structural model could explain 33.5% of the variance for intended use. This greatly exceeded 10%, which was suggested by Falk and Miller [73] as an indication of substantive explanatory power.

As shown in Figure 2, all hypotheses were supported except H6 (Organizational Structural Assurance → Trust). In support of H1 and H2, the results indicate that familiarity with the vendor of P2P sharing software and reputation of the vendor of P2P sharing software were positively related to trusting beliefs. H3 and H4 postulate the influences of peer-network situational normality and organizational situational normality on trusting beliefs. In support of H3 and H4, the positive relationships between peer-network and organizational situational normality and trusting beliefs were found significant. Regarding the influences of structural assurances on trusting beliefs, peer-network structural assurance was positively related to trusting beliefs (H5 was supported); but organizational structural assurance did not have significant impact on trusting beliefs (H6 was not supported). Trusting beliefs were negatively related to perceived risks (H7 was supported); perceived risks were found to be negatively related to intended use

[2]The reward was framed in Singapore dollars. One Singapore dollar was around 59 US cents at the time of experiment.

Table 1. Psychometric properties of the measurement model.

Construct indicators	Factor loadings	Composite reliability	Cronbach's alpha	Variance extracted
Intention to use (INT)				
INT1	0.983	0.986	0.873	0.959
INT2	0.984			
INT3	0.970			
Perceived risk (RISK)				
RISK1	0.976	0.949	0.889	0.862
RISK2	0.889			
RISK3	0.918			
Trust in P2P Vendor (TRU)				
TRU1	0.939	0.892	0.837	0.735
TRU2	0.805			
TRU3	0.822			
Reputation (VR)				
VR1	0.898	0.916	0.886	0.783
VR2	0.859			
VR3	0.898			
Familiarity (FV)				
FV1	0.921	0.912	0.899	0.776
FV2	0.896			
FV3	0.822			
Organizational structural assurances (OSA)				
OSA1	0.912	0.880	0.811	0.712
OSA2	0.890			
OSA3	0.715			
Organizational situational normality (OSN)				
OSN1	0.717	0.858	0.878	0.670
OSN2	0.820			
OSN3	0.908			
Peer-network structural assurances (PSA)				
PSA1	0.905	0.929	0.865	0.814
PSA2	0.924			
PSA3	0.877			
Peer-network situational normality (PSN)				
PSN1	0.889	0.913	0.850	0.778
PSN2	0.862			
PSN3	0.894			

Table 2. Discriminant validity.

	VR	FV	OSA	OSN	PSA	PSN	TRU	RISK	INT
VR	0.885								
FV	0.604	0.881							
OSA	0.547	0.585	0.844						
OSN	0.379	0.185	0.300	0.812					
PSA	0.467	0.364	0.422	0.261	0.902				
PSN	0.433	0.378	0.460	0.309	0.378	0.882			
TRU	0.590	0.578	0.470	0.361	0.458	0.467	0.857		
RISK	0.100	0.119	0.335	0.287	0.022	0.106	−0.351	0.928	
INT	0.253	0.086	0.008	0.513	0.128	0.260	0.389	−0.217	0.979

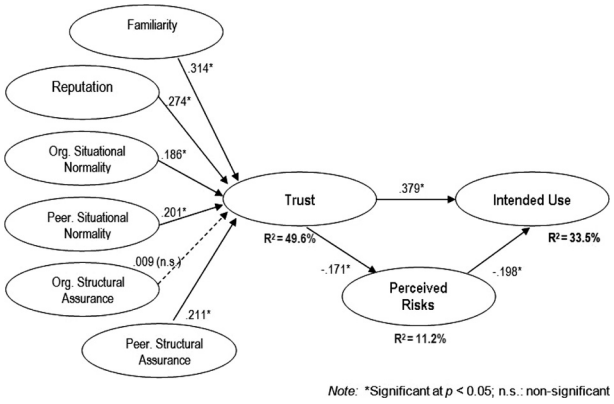

Figure 2. Structural model.

(H8 was supported); trusting beliefs were positively related to intended use (H9 was supported).

5. Discussion

Social computing focuses on how users may have more autonomy to express their ideas and participate in social exchanges in various ways, one of which may be P2P file sharing. While technical issues are still relevant from a social computing perspective, this research examines P2P file sharing from a more social perspective to understand how factors influencing individuals in groups or networks affect their online behaviors. The results show that experienced users' continued use of P2P sharing software depends on both trust beliefs in the software vendor and risk perceptions associated with P2P sharing. Most prior research on trust has reported knowledge-based factors, cognitive factors, and institutional factors as significant determinants of trusting beliefs. Our results confirmed the effects of these trust antecedents in a social computing context. In addition, this research has differentiated two components of institutional trust: the organizational structures and the peer-network structures. Our results showed that the organizational structures were overshadowed when peer-network structures, knowledge-based trust, and cognitive trust were also assessed. Specifically, the proposed organizational structural assurances did not have impact on trust in P2P vendor. A possible explanation for this could be that the survey participants are not aware of the existence of any legal protection or not familiar with the industry's self-regulation body. In fact, none of the survey respondents lastly used a P2P sharing software that is provided by a member vendor in P2P United [43].

Our preliminary findings have several practical implications in the P2P landscape. First, this study highlights the important roles of P2P vendors and peer network in building effective online communities. As discussed earlier, building trustworthy dependency on other peers is difficult due to high uncertainties of peers. Peer-to-peer vendors, therefore, should contribute to provide functions into the sharing software to build a safe, effective, and stable P2P network that can lead to users' perception of peer-network situational normality and structure assurance [74]. P2P vendors should also actively take efforts in addressing such issues like free-riding, content piracy, malicious computer attack, rather than passively leaving these issues as they were and merely playing a role as software provider. This is also supported by the call for the self-regulation in P2P industry by researchers [8] and by lawmakers [56]. In practice, more and more P2P software vendors are implementing such mechanisms, like providing peers with incentives for opening more shares in exchange for faster download speed, and offering the accounting functions in the software to protect against malicious users. Second, reputation of the vendor and user familiarity with the vendor should also be actively promoted, e.g. via promoting the new features and procedures of the software through mass media. Third, both organizational and peer-network situational normality, such as a typical user interface, and effective mechanisms like free-riding prevention and anti-flooding, are important strategies for trust building.

Organizational structural assurances were shown not important in trust building by our data analysis. This insignificant effect is probably due to the participants' lack of knowledge about available organizational safeguards. One interpretation of this result is that, users of social computing applications increasingly take trust cues from one another or from communities rather than from organizational sources. As such, user communities are increasingly driving innovations and communications from the bottom-up, and the information flow, economic value, and power are starting to shift from organizations to user communities. This interpretation is in line with the trends discussed in the Introduction per researchers' observations [2, 4].

6. Conclusion

P2P networks do not merely implement Web-based interfaces but also they design architectures that allow peer wise communication and social action; that is, P2P networks imply communities as well as sophisticated enabling technologies [3]. This exploratory study seeks to understand what steps can be taken to increase users' trust beliefs and reduce their risk perceptions so as to encourage legitimate interactions in social computing platforms. Our results can also be applied to users who do not have initial experiences, as the information about the vendor's trustworthiness and the level of perceived risk can be passed on to and propagated among initial users and affect their adoption of P2P sharing software [75]. Although the data generally support the proposed model, caution must be exercised when generalizing these findings. This study was conducted in Singapore,

care must be taken when generalizing these findings to consumers in other social, economic, and cultural environments, and future research should attempt to replicate this study in other countries, especially those in North America and in Europe, to further validate the research model. Most P2P sharing networks are running globally over the Internet, and the legal risks presented in one country may be absent in other countries. How to effectively prevent global P2P users from sharing and downloading copyright violated materials? Who will play the most important role in regulating the usage behavior in using P2P sharing software? These would be fruitful questions for future research.

Through the causal modeling of the antecedents affecting use intentions, our findings provide preliminary empirical support to understand trust and risk issues in the context P2P file sharing networks. Nevertheless, since some characteristics of this study may limit the generalizability of our findings, several avenues for future work remain. We hope this study makes a modest contribution to stimulating further research in the field of the P2P file sharing networks.

Appendix A.

Measurement items (measured on 7-point Likert-type scale).

Intended use (INT): (Pavlou and Gefen [33])
INT1 I intend to continue using the P2P file sharing software to search for, download or share resources.
INT2 I predict I would continue using the P2P file sharing software.
INT3 I plan to continue using the P2P file sharing software.

Perceived risk (RISK): (Pavlou and Gefen [33])
RISK1 There is a high potential for loss involved in using the P2P file sharing software.
RISK2 There is a considerable risk involved in using the P2P file sharing software to search for, download and/or share resources.
RISK3 My decision to use the P2P file sharing software is risky.

Trust in P2P vendor (TRU): (Gefen *et al.* [59])
TRU1 I believe the vendor is honest.
TRU2 I believe the vendor cares about its users.
TRU4 I believe the vendor is reliable.

Reputation (VR): (McKnight *et al.* [5])
VR1 The vendor has a reputation for being honest.
VR2 The vendor has a reputation for being concerned about the users.
VR3 Most users think that this vendor has a reputation for being fair.

Familiarity (FV): (Gefen *et al.* [59])
FV1 I am familiar with the vendor through resource searching and download by the P2P file sharing software.
FV2 I am familiar with the vendor through sharing resources to other peers by the P2P file sharing software.
FV3 I am familiar with the vendor through reading magazine/newspaper articles or ads.

Peer-network structural assurances (PSA): (McKnight *et al.* [5])
PSA1 The peer-network has enough safeguards to make me feel comfortable transferring and sharing resources with other peers.
PSA2 I feel assured that the technological structures adequately protect me from peers' opportunistic behaviors.
PSA3 I feel assured that other peers cannot free ride on my shared resources.

Peer-network situational normality (PSN): (McKnight *et al.* [5])
Based on your experiences with peers whom you have downloaded resources from, or shared resources to, among those peers:
PSN1 Most peers are in general predictable and consistent regarding their behaviors.
PSN2 Most peers are trustworthy in transferring and sharing resources with other peers.
PSN3 Most peers are reliable to download resources from, and/or share resources to.

Organizational structural assurances (OSA): (Gefen *et al.* [59])
OSA1 I feel assured that downloaded resources are legal because the vendor provides statements of guarantees that all shared resources are legal.
OSA2 I feel safe using the P2P sharing software because the vendor is on the list of P2P United.
OSA3 I am comfortable searching, downloading or sharing resources because of the regulatory and technological structures built by the vendor.

Organizational situational normality (OSN): (Gefen *et al.* [59])
Based on your experiences with other similar P2P sharing software...

(continued on next page)

Appendix A. Continued.

Intended use (INT): (Pavlou and Gefen, 2004)	
OSN1	The mechanisms built into the software to encourage peers to download/share resources are typical of other similar P2P file sharing software.
OSN2	The steps required to search for, download and share resources are typical of other similar P2P file sharing software.
OSN3	The approach used by the software to encourage peers to download/share resources is the type of approach most similar P2P sharing software employs.

Acknowledgements. The authors would like to thank Hao Wang and Audrey Lim at the Pennsylvania State University for their assistance on an earlier version of this paper.

References

[1] Parameswaran, M. and Whinston, A.B. (2007) Social computing: an overview. *Commun. Assoc. Inf. Syst.* **19**: 762–780.

[2] Ip, R. and Wagner, C. (2008) Weblogging: a study of social computing and its impact on organizations. *Decis. Support Syst.* **45**(2): 242–250.

[3] Wang, F.Y., Carley, K.M., Zeng, D. and Mao, W. (2007) Social computing: from social informatics to social intelligence. *IEEE Intell. Syst.* March/April: 79–83.

[4] Charron, C., Favier, J. and Li, C. (2006) *Social Computing: How Networks Erode Institutional Power, and What to Do About It* (Forester Research). Retrieved 26 May 2011, from http://www.forrester.com/Research/Document/Excerpt/0,7211,38772,00.html.

[5] McKnight, D.H. and Chervany, N.L. (2002) What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology. *Int. J. Electron. Com.* **6**(2): 35–59.

[6] Hoffman, D.L., Novak, T. and Peralta, M.A. (1999) Information privacy in the marketspace: implications for the commercial uses of anonymity on the Web. *Inf. Soc.* **15**(2): 129–139.

[7] Dholakia, U.M., Bagozzi, R.P. and Pearo, L.K. (2004) A social influence model of consumer participation in network- and small-group-based virtual communities. *Int. J. Res. Marketing* **21**(3): 241–263.

[8] Hughes, J., Lang, K.R. and Vragov, R. (2008) An analytical framework for evaluating peer-to-peer business models. *Electron. Com. Res. Appl.* **7**(1): 105–118.

[9] Schoder, D. and Fischbach, K. (2003) Peer-to-peer prospects. *Commun. ACM* **46**(2): 27–29.

[10] Mcguire, D. (2004) *Lawmakers Push Prison for Online Pirates.* Retrieved 26 May 2011, from http://www.washingtonpost.com/wp-dyn/articles/A40145-2004Mar31.html.

[11] Dingledine, R., Freedman, J.M. and Molnar, D. (2001) Accountability. In Oram, A. [ed.] *Peer-to-Peer: Harnessing the Power of Disruptive Technologies* (Cambridge, MA: O'Reilly & Associates), 271–339.

[12] Reiter, M.K. and Rubin, A.D. (1999) Anonymous Web transactions with crowds. *Commun. ACM* **42**(2): 32–38.

[13] Tsivos, P., Whitley, A.E. and Hosein, I. (1999) An exploration of the emergence, development and evolution of regulatory characteristics of information systems. In *Proceedings of the Twentieth International Conference on Information Systems (ICIS)* (Charlotte, NC), 813–816.

[14] Borland, J. (2003) *Fingerprinting P2P pirates.* Retrieved 26 May 2011, from http://news.com.com/2100-1023_3-985027.html.

[15] Havlena, W.J. and Desarbo, W.S. (1991) On the measurement of perceived consumer risk. *Decis. Sci.* **22**(4): 927–939.

[16] Ganesan, S. (1994) Determinants of long-term orientation in buyer–seller relationships. *J. Marketing* **58**: 1–19.

[17] Yates, J.F. and Stone, E.R. (1992) Risk appraisal. In Yates, J.F. [ed.] *Risk-Taking Behavior* (Chichester, UK: John Wiley & Sons), 49–85.

[18] Jarvenpaa, S.L. and Tractinsky, N. (1999) Consumer trust in an Internet store: a cross-cultural validation. *J. Comput. Mediated Commun.* **5**(2): 1–35.

[19] Peter, J.P. and Tarpey, S.L.X. (1975) A comparative analysis of three consumer decision strategies. *J. Consum. Res.* **2**(1): 29.

[20] Moon, Y. (2000) Intimate exchanges: using computers to elicit self-disclosure from consumers. *J. Consum. Res.* **26**: 323–339.

[21] Stewart, K.J. (2003) Trust transference on the world wide Web. *Organ. Sci.* **14**(1): 5–17.

[22] Pew-Internet, American-Life-Project (2004) *The State of Music Downloading and File-Sharing Online.* Retrieved 26 May 2011, from http://www.pewinternet.org/~/media//Files/Reports/2004/PIP_Filesharing_April_04.pdf.pdf.

[23] Pavlov, V.O. and Saeed, K. (2003) A resource-based assessment of the gnutella file-sharing network. In *Proceedings of 24th Annual International Conference on Information Systems (ICIS)* (Seattle, WA), 85–95.

[24] Lewicki, R. and Bunker, B.B. (1995) Trust in relationships: a model of trust development and decline. In Bunker, B.B. and Rubin, J.Z. [eds.] *Conflict, Cooperation, and Justice* (San Francisco, CA: Jossey-Bass), 133–173.

[25] Lewis, J.D. and Weigert, A.J. (1985) Trust as a social reality. *Soc. Forces* **63**(4): 967–985.

[26] Lane, C. and Bachmann, R. (1996) The social constitution of trust: supplier relations in Britain and Germany. *Organiz. Stud.* **17**(3): 365–395.

[27] Moorman, C., Desphande, R. and Zaltman, G. (1993) Factors affecting trust in market research relationships. *J. Marketing* **57**(1): 81–101.

[28] Luhmann, N. (1988) Familiarity, confidence, trust: problems and alternatives. In Gambetta, D.G. [ed.] *Trust* (New York: Basil Blackwell), 94–107.

[29] Grabner-Kräuter, S. and Kaluscha, E.A. (2003) Empirical research in online trust: a review and critical assessment. *Int. J. Hum. Comput. Stud. Special Issue on 'Trust and Technology'* **58**(6): 783–812.
[30] McKnight, D.H., Cummings, L.L. and Chervany, N.L. (1998) Initial trust formation in new organizational relationships. *Acad. Manage. Rev.* **23**(3): 472–490.
[31] McKnight, D.H., Choudhury, V. and Kacmar, C. (2002) Developing and validating trust measures for e-commerce: an integrative typology. *Inf. Syst. Res.* **13**(3): 334–359.
[32] Gefen, D., Karahanna, E. and Straub, D.W. (2003) Trust and TAM in online shopping: an integrated model. *MIS Q.* **27**(1): 51–90.
[33] Pavlou, P.A. and Gefen, D. (2004) Building effective online marketplaces with institution-based trust. *Inf. Syst. Res.* **15**(1): 37–59.
[34] Bhattacherjee, A. (2002) Individual trust in online firms: scale development and initial test. *J. Manage. Inf. Syst.* **19**(3): 211–241.
[35] Kollock, P. (1999) The production of trust in online markets. *Adv. Group Processes* **16**: 99–123.
[36] Lee, J. (2003) An end-user perspective on file-sharing systems. *Commun. ACM* **46**(2): 49–53.
[37] Giffin, K. (1967) The contribution of studies of source credibility to a theory of interpersonal trust in the communication process. *Psychol. Bull.* **68**(2): 104–120.
[38] Luhmann, N. (1979) *Trust and Power* (Chichester, UK: John Wiley & Sons).
[39] Li, X., Hess, T.J. and Valacich, J.S. (2008) Why do we trust new technology? A study of initial trust formation with organizational information systems. *J. Strategic Inf. Syst.* **17**(1): 39–71.
[40] Grazioli, S. and Wang, A. (2001) Looking without seeing: Understanding unsophisticated consumers' success and failure to detect Internet deception. In *Proceedings of the International Conference on Information Systems (ICIS)* (New Orlean, LA), 193–204.
[41] Shapiro, D.L., Sheppard, B.H. and Cheraskin, L. (1992) Business on a handshake. *Negotiation J.* **3**: 365–377.
[42] Zucker, L.G. (1986) Production of trust: institutional sources of economic structure, 1840–1920. In Staw, B.M.A and Cummings, L.L. [eds.] *Research in Organizational Behavior* (Greenwich, CT: JAI Press), 53–111.
[43] P2P United. (2004) *P2P United: Fighting for the Future of Peer-to-Peer Technology.* Retrieved 26 May 2011, from http://www.ftc.gov/bcp/workshops/filesharing/presentations/eisgrau.pdf.
[44] Mayer, R.C., Davis, J.H. and Schoorman, F.D. (1995) An integration model of organizational trust. *Acad. Manage. Rev.* **20**(3): 709–734.
[45] Samant, K. (2003) Free riding, altruism, and cooperation on peer-to-peer file-sharing networks. In *Proceedings of 24th Annual International Conference on Information Systems (ICIS)* (Seattle, WA), 914–920.
[46] Kwok, S.H. and Yang, C.C. (2004) Searching the peer-to-peer networks: the community and their queries. *J. Am. Soc. Inf. Sci. Technol.* **55**(9): 783–793.
[47] Borland, J. (2002) *Start-Ups Try to Dupe File-Swappers* (CNET News.Com). Retrieved 26 May 2011, from http://news.com.com/2100-1023-943883.html.
[48] Levine, D. (2002) *Not the Real Slim Shady.* Retrieved 26 May 2011, from http://dir.salon.com/story/tech/feature/2002/06/10/eminem_mp3/index.html.
[49] Lee, K.C., Kang, I.W. and McKnight, D.H. (2007) Transfer from offline trust to key online perceptions: an empirical study. *IEEE Trans. Eng. Manage.* **54**(4): 729–741.
[50] Pennington, R., Wilcox, H.D. and Grover, V. (2003) The role of system trust in business-to-consumer transactions. *J. Manage. Inf. Syst.* **20**(3): 197–226.
[51] Baier, A. (1986) Trust and antitrust. *Ethics* **96**: 231–260.
[52] Garfinkel, H. (1963) A conception of, and experiments with, 'trust' as a condition of stable concerted actions. In Harvey, O.J. [ed.] *Motivation and Social Interaction* (New York: Ronald Press), 187–238.
[53] Shapiro, S.P. (1987) The social control of impersonal trust. *AJS* **93**: 623–658.
[54] Palmer, J.W., Bailey, J.P. and Faraj, S. (2000) The role of intermediaries in the development of trust on the WWW: The use and prominence of trusted third parties and privacy statements. *J. Comput. Mediated Commun.* **5**.
[55] Oram, A. (2001) *Peer-to-Peer: Harnessing the Power of Disruptive Technologies* (Cambridge, MA: O'Reilly & Associates).
[56] Borland, J. (2003) *Senators Ask P2P Companies to Police Themselves* (CNET News.com). Retrieved 26 May 2011, from http://news.com.com/2100-1028_3-5110785.html.
[57] Waldman, M., Cranor, F.L. and Rubin, A. (2001) Trust. In Oram, A. [ed.] *Peer-to-Peer: Harnessing the Power of Disruptive Technologies* (Cambridge, MA: O'Reilly & Associates), 242–270.
[58] Johnson, L.J. and Cullen, B.J. (2002) Trust in cross-cultural relationships. In Gannon, M.J. and Newman, K.L. [eds.] *The Blackwell Handbook of Cross-Cultural Management* (Oxford, UK and Malden, MA: Blackwell), 335–360.
[59] Gefen, D., Rao, V.S. and Tractinsky, N. (2003) The conceptualization of trust, risk and their relationship in electronic commerce: the need for clarifications. In *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS)* (Big Island, HI), 192–201.
[60] Ajzen, I. (1985) From intentions to actions: A theory of planned behavior. In Kuhl, J. and Beckmann, J. [eds.] *Action Control: From Cognition to Behavior* (New York, NY: Springer Verlag), 11–39.
[61] Ajzen, I. (1991) The theory of planned behavior. *Organiz. Behav. Hum. Decis. Processes* **50**: 179–211.
[62] Gefen, D. (2002) Customer loyalty in e-commerce. *J. Assoc. Inf. Syst.* **3**: 27–51.
[63] Pavlou, P.A. (2003) Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *Int. J. Electron. Com.* 7(3): 69–103.
[64] Churchill, G.A. (1979) A paradigm for developing better marketing constructs. *J. Marketing Res.* **16** (February): 64–73.
[65] Moore, G.C. and Benbasat, I. (1991) Development of an instrument to measure the perceptions of adopting an information technology innovation. *Inf. Syst. Res.* **2**(3): 173–191.
[66] Fornell, C. and Bookstein, F.L. (1982) Two structrual equation models: lisrel and pls applied to customer exit-voice theory. *J. Marketing Res.* **19**(11): 440–452.

[67] Chin, W.W. (1998) The partial least squares approach to structural equation modeling. In Marcoulides, G.A. [ed.] *Modern Methods for Business Research* (London: Psychology Press), 295–336.
[68] Kim, D. and Benbasat, I. (2006) The effects of trust-assuring arguments on consumer trust in Internet stores: application of Toulmin's model of argumentation. *Inf. Syst. Res.* **17**(3): 286–300.
[69] Cook, M. and Campbell, D.T. (1979) *Quasi-Experimentation: Design and Analysis Issues for Field Settings* (Boston, MA: Houghton Mifflin).
[70] Chin, W.W. (1998) The partial least squares approach to structural equation modeling. In Marcoulides, G.A. [ed.] *Modern Methods for Business Research* (Mahwah, NJ: Lawrence Erlbaum Associates), 295–336.
[71] Nunnally, J.C. (1978) *Psychometric Theory* (New York: McGraw-Hill), 2nd ed.
[72] Campbell, D.T. and Fiske, D.W. (1959) Convergent and discriminant validation by the multitrait–multimethod matrix. *Psychol. Bull.* **56**(1): 81–105.
[73] Falk, R.F. and Miller, N.B. (1992) *A Primer for Soft Modeling* (Akron, OH: University of Akron Press).
[74] Aringhieri, R., Damiani, E., Vimercati, S.D.C.D., Paraboschi, S. and Samarati, P. (2006) Fuzzy techniques for trust and reputation management in anonymous peer-to-peer systems. *J. Am. Soc. Inf. Sci. Tech.* **57**(4): 528–537.
[75] Song, J. and Walden, A.E. (2003) Consumer behavior in the adoption of peer-to-peer technologies: an empirical examination of information cascades network externalities. In *Ninth Americas Conference on Information Systems (AMCIS)* (Tampa, FL), 1801–1810.